ENHANCED SECURE KEYWORD SEARCH AND DATA SHARING MECHANISM FOR CLOUD COMPUTING

[#1]ASHRITHA KUDIDILA,
[#2]SATHVIKA GANDESRI,
[#3]S.NAVEEN KUMAR, ***Associate Professor,***
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: The growth of cloud infrastructure has resulted in significant cost savings for computer infrastructure hardware and software solutions. To preserve the integrity of data, information is sometimes safeguarded before being transmitted to the cloud. Encrypted knowledge is more difficult to locate and exchange than unencrypted information. However, this is the responsibility of the cloud service provider, as clients rely on the cloud to run fast queries and deliver results while maintaining data security. To overcome these concerns, we suggest encrypting cloud data using a ciphertext-policy attribute-based technique that includes keyword search and information sharing (CPAB-KSDS). The proposed approach allows you to do both: search for keywords based on attributes and send information based on attributes, as opposed to alternative systems that only support one of the two possibilities. In addition, if we do not engage with the PKG in the sharing area, the keyword in our theme may change. This essay also addresses the CPAB-KSDS concept and the corresponding security model. Furthermore, we usually suggest a specific theme and demonstrate that it is secure against chosen ciphertext and chosen keyword attacks in the random oracle model. As its characteristics and performance are tested, it becomes clear that the proposed structure is both practical and economical.

Keywords:Hardware and software solutions,data security,CPAB-KSDS

I. INTRODUCTION

CLOUD COMPUTING

Cloud computing is the use of computer resources, such as software and tools, that are delivered as a service across a network, usually the Internet. The term "cloud" is used in diagrams to describe the intricate architecture of a system that resembles a cloud. Cloud computing allows users to outsource data, code, and processes to remote servers. Cloud computing is the shared use of software and hardware resources intended for internet-based operations. Following that, a third party distributes these resources as managed services for public use. These services usually provide access to complex server networks and code-intensive applications.

CLOUD COMPUTING WORKS

Cloud computing, which uses outmoded supercomputing technology traditionally reserved for research institutes and the military, allows consumer-oriented applications such as extremely realistic video games, financial portfolios, and data storage to execute billions of computations per second.

In cloud computing, data processing is spread across large networks of computer clusters. These networks often use regular computer hardware and customized connections. The shared IT infrastructure is made up of a large number of interconnected systems. Virtualization techniques are widely used to improve the versatility of cloud computing.

Characteristics and Services Models:

A section of the National Institute of Standards and Technology (NIST) has produced the following publicly available definitions of cloud computing to support its core features:

On-demand self-service: Customers can reserve computer resources like server time and network storage without having to contact each service provider individually. This can be accomplished independently and without delay.

Broad network access: The features unit is available for purchase on the internet and may be accessed via outmoded devices that appeal to a wide range of consumers, including those who are thin or thick, such as laptops, PDAs, and smartphones.

Resource pooling: The service provider uses a multitenant technique to allocate computer resources across multiple clients. This architecture ensures that each customer has access to movable physical and virtual resources according to their individual needs. This method offers a degree of location independence by allowing the user to choose a higher-level location, such as a data center, country, or state. Nonetheless, the user usually lacks power or access to accurate information about the location of the services. Resource types include storage, compute capacity, memory, network metrics, and virtual machines.

fast elasticity: A capacity is a unit of measurement that can be quickly and easily changed to increase or decrease in magnitude, and in some situations even by itself. Customers often believe that provisioning powers are highly adjustable and easily available for purchase in any quantity and at any time.

II.LITERATURE SURVEY

1) Fuzzy identity-based cryptography

AUTHORS: A. Sahai and B. Waters

Our contribution to the field of Identity-Based Cryptography (IBE) is known as "fuzzy identity-based cryptography." An Associate in Nursing identity is often defined as a set of describing features in fuzzy IBE. Fuzzy Identity-Based Encryption (IBE) allows an entity (ω) to have a private key that can decipher ciphertext encrypted with ω ′, as long as ω and ω ′ are significantly connected using the "set overlap" distance metric. The use of biometric data as identities within a Fuzzy IBE framework will increase cryptography. The deployment of biometric IDs becomes more convenient, despite their vulnerability to modification throughout the sampling method, thanks to the error-handling capabilities of a Fuzzy IBE system. Furthermore, we intend to demonstrate Fuzzy-IBE's applicability to a specific type of application known as "attribute-based encryption."

This study looks at two separate types of inaccurate Identity-Based Encryption (IBE) architectures. Our breakthroughs will be known as identity-based cryptography. This method comprises concealing a message using a number of attributes that compose a faulty identity. Our IBE schemes are designed to tolerate flaws and are not vulnerable to joint efforts. We do not use arbitrary oracles in our fundamental architecture. To demonstrate the functionality of our techniques, we usually use the Selective-ID security paradigm.

2)Ciphertext-PolicyAttribute-Based cryptography

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters

Only individuals with specified credentials or traits should be permitted access to information within dispersed systems. Currently, the only way to enforce these requirements is to keep the data on a secure server and control access to it through that server. However, if any of the servers storing the information are compromised, the data's confidentiality will be threatened. We find this study's description of a way for enabling more advanced access control to protected data useful. To implement attribute-based cryptography, ciphertext principles must be followed. Even if there is a problem with the storage service, our protocols ensure that encrypted data remains secret and secure. Our processes are also resistant to collusion attempts. Previously, attribute-based encryption systems used attributes to decode data, and policies were embedded in user keys. Our method establishes the World Health Organization's strategy for decrypting information using encryption, whereas earlier systems used attributes to provide explanations for encrypted data. As a result, our techniques have some similarities to more widely used access control systems, such as role-based access control (RBAC). System execution and performance evaluation are part of our Associate of Nursing curriculum.

3) Privacy-preserving personal health record exploitation multi-authority attribute-based cryptography with revocation

AUTHORS: H. Qian, J. Li, Y. Zhang, and J. Han

Personal Health Record (PHR) services are a new and quickly developing tool for nurses to exchange health information. Internet-connected Personal Health Record (PHR) solutions enable people to manage and control their own health data and information. Third-party storage of personal health records (PHRs) is common, and cloud service providers frequently facilitate this practice. However, cloud services can be particularly harmful to privacy since they provide cloud service providers or unauthorized parties access to sensitive data, such as personal health records (PHRs). Implementing attribute-based cryptography (ABE) allows users to securely and flexibly limit access to cloud-stored patient health records. However, other challenges have to be addressed, such as the installation of precise access control, the quantification of key management, and the prompt and cost-effective revocation of user credentials. The goal of this project is to create a Personal Health Record (PHR) system that protects confidentiality, allows for accurate access management, and permits cost-effective revocation. Our multi-authority attribute-based encryption (ABE) system allows for dynamic policy switching and low-cost revocation of users or attributes on demand. This allows us to accurately and precisely restrict access to protected health records (PHRs). The majority of our debate is around worries regarding the storage and encryption of patient health records on systems that are only partially trusted, as well as the massive amount of information about homeowners. Our theme's access structure is a communicatory tree, and to improve its security, we will use the Diffie-Hellman assumption.

III. METHODOLOGY

Java technology

Java technology includes both a computer language and a software platform. Java is a programming language. The aforementioned expressions all apply to the computer language Java. It will almost probably be application-focused. To run a program on a laptop, you must either build it or interpret it in one of the most popular programming languages. One distinguishing feature of the Java programming language is the ability to interpret and compile programs at any time. The translator is originally used to translate a program to Java bytecode, which is an intermediate language. These codes are platform neutral and can be interpreted by the Java interpreter. The laptop's interpreter reads and executes all instructions in the Java memory device unit code. Interpretation occurs when a program terminates, whereas compilation occurs only once. The accompanying illustration explains how this works.

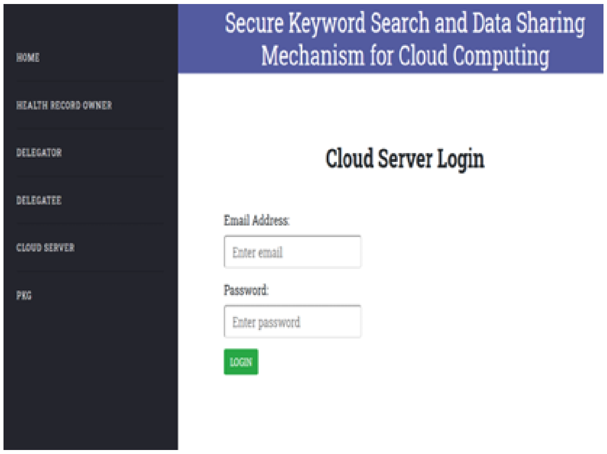
SQL

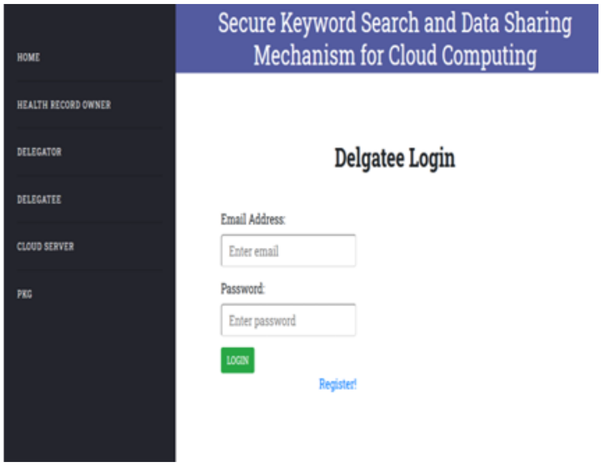
SQL can be used to manage data streams in a real-time data stream management system (RDSMS) or to manipulate data in a relational database management system (RDBMS). Working with structured data, which is made up of relationships between variables and objects, is especially useful. When compared to previous read-write APIs like ISAM or VSAM, SQL has two major advantages. Initially, the concept of accessing several documents using a single word was proposed. Furthermore, it eliminates the need to explain the technique for correctly retrieving a record, regardless of whether a linked index is used. A large number of statements contain SQL. Their sources include relational mathematics and tuple relational calculus. These statements are part of the information manipulation language (DML), data management language (DCL), information search language (DQL), and information description language (DDL).SQL may define information (by creating and amending models), edit information (by adding, changing, and removing entries), and control access to information. SQL, although being a declarative language, includes automated components.

IV. IMPLEMENTATION

MODULES:

- Health Record owner
- Delegator
- Delegate
- Cloud Server
- PKG



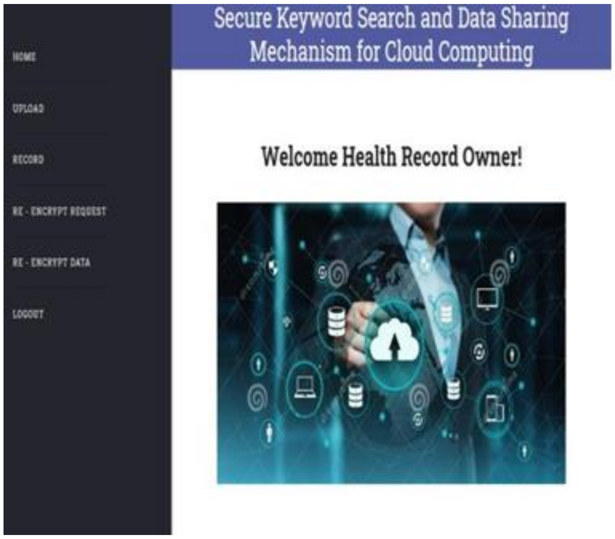


Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

Delgatee Login

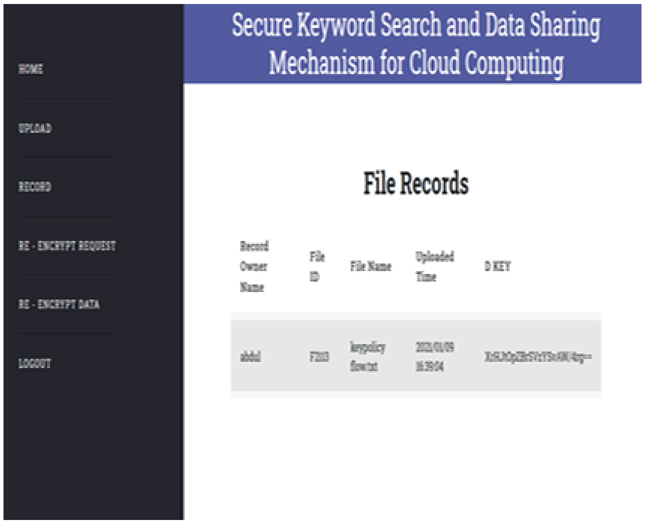
Email Address: Enter email

Password: Enter password



Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

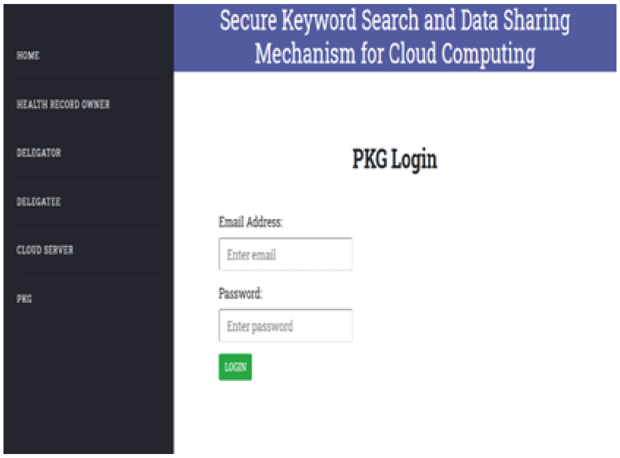
Welcome Health Record Owner!



Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

File Records

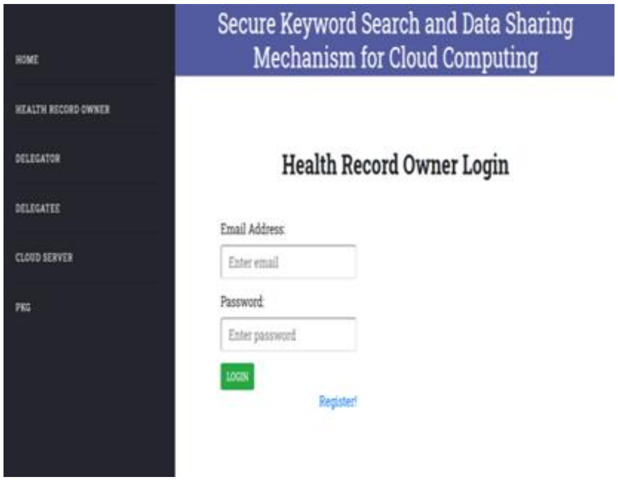
Record Owner Name	File ID	File Name	Uploaded Time	D KEY
abdul	F203	keypolicy flow.txt	2021/01/09 16:39:04	XrSLROpZBrSVzYSx4M/4rg==


Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

PKG Login

Email Address: Enter email

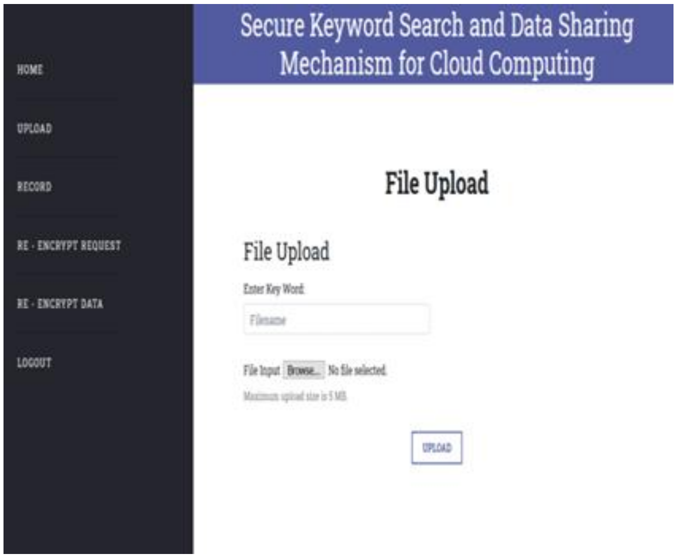
Password: Enter password


Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

Health Record Owner Login

Email Address: Enter email

Password: Enter password


Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

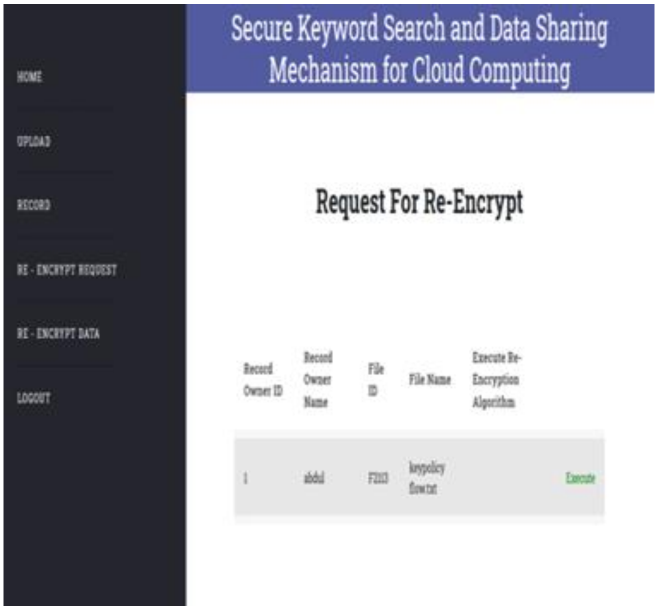
File Upload

File Upload

Enter Key Word: Filename

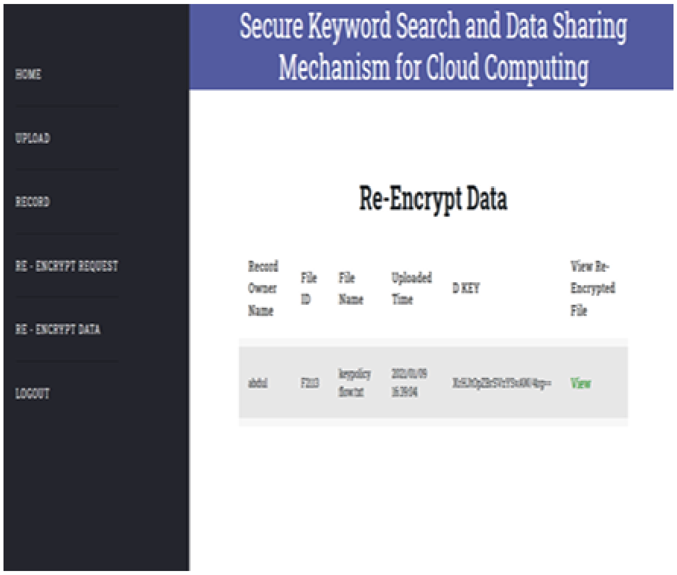
File Input Browse... No file selected.

Maximum upload size is 5 MB.


Secure Keyword Search and Data Sharing Mechanism for Cloud Computing
HOME
UPLOAD
RECORD
RE - ENCRYPT REQUEST
RE - ENCRYPT DATA
LOGOUT

Request For Re-Encrypt

Record Owner ID	Record Owner Name	File ID	File Name	Execute Re-Encryption Algorithm
1	abdul	F2113	keypolicy flow.txt	Execute


Secure Keyword Search and Data Sharing Mechanism for Cloud Computing
HOME
UPLOAD
RECORD
RE - ENCRYPT REQUEST
RE - ENCRYPT DATA
LOGOUT

Re-Encrypt Data

Record Owner Name	File ID	File Name	Uploaded Time	D KEY	View Re-Encrypted File
abdul	F2113	keypolicy flow.txt	2021/01/09 16:39:04	XsS3tQpZbSVtY5x4M4qp=	View

MODULES DESCRIPTION:

Health Record Owner:

To access the Health Record Owner module, users must first complete the registration process. After properly enrolling, the person whose record you own gains access to the system and can use encrypted keywords and hashing algorithms to send data to the cloud server. The ability to examine objects uploaded to the cloud is extensively established. The owner of the health record can either permit or refuse the data user access to the desired file. After the request is approved, the data proprietor will send the proof object and secret key via mail service.

Delegator:

Prior to using the Delegator module, users must give sensitive information. Following that, individuals must enter a secret key to prove their identity each time they log in. The individual in charge of health information may search any file that the proprietor sends to them. An individual may submit a formal request for access to the information, which will be forwarded to the appropriate parties that have the health records.

Delegate:

If the health record owner provides permission, the delegate can acquire the secret key, proof object, and decryption key by registered mail.

Cloud Server (CS):

The Cloud Server module allows the Cloud Provider to thoroughly inspect each file's specs. Each data analysis is accessible through the cloud.

PKG:

The PKG utility allows you to see information about both the delegator and the delegate.

V. CONCLUSION

This paper presents a unique strategy dubbed the ciphertext-policy attribute-based method (CPAB-KSDS), which intends to improve data sharing and keyword searches. The fundamental goal of this research is to create a technology called concrete CPAB-KSDS. One of the key goals is to demonstrate the system's effectiveness in protecting CCA security during a random Oracle scenario. The examination of properties and performance shows that the proposed method is both functional and favorable. The difficult challenge of combining keyword search and data sharing capabilities with attribute-based encryption during the sharing phase without the use of a Public Key Generator (PKG) has been completed. Furthermore, our methodology raises exciting unresolved questions, such as inventing a novel method to improve the comprehensiveness of keyword queries or developing the CPAB-KSDS scheme without relying on arbitrary oracles.

REFERENCES

1. Agarwal, Mohit & Singh, Abhishek &Arjaria, Gautama Siddhartha & Sinha, Amit & Gupta, Suneet. (2020). ToLeD: herb malady Detection pattern Convolutional Neural Network. Procedia subject field. 167. 293-301. 10.1016/j.procs.2020.03.225
2. P. Tm, A. Pranathi, K. SaiAshritha, N. B. Chittaragi and S. G. Koolagudi, "Tomato disease Detection pattern Convolutional Neural Networks," 2018 Eleventh International Conference on trendy Computing (IC3), 2018, pp. 1-5, doi: 10.1109/IC3.2018.8530532.